

EC441: Lab 6

Daniel Andronov

Monday 21st November, 2016

6.0 Prelab

Problem 4.5

Part a)	Prefix	Interface
	224.0.0.0	0
	224.64.0.0	1
	224.65.0.0	2
	225.64.0.0	3
	else	4

- Part b)
- i) 200.145.81.85 matches no prefix and is sent to interface 3
 - i) 225.64.195.60 matches 225.0.0.0 the most and is sent to interface 1
 - i) 225.128.17.119 matches no prefix and is sent to interface 3

Problem 4.6	Range	Interface
	0 - 63	0
	64 - 95	1
	96 - 127	2
	128 - 192	3
	192 - 255	4

Problem 4.8 Subnet 1 needs 12 interfaces which requires 3 bits. Subnets 2 need 60 interfaces or 6 bits and Subnet 3 needs 7 bits for 90 interfaces.

Subnet	Network Address
1	223.1.170.240/3
2	223.1.17.192/6
3	223.1.17.128/9

Problem 4.17

- Part a) Capture packets & continually update the max range of the IDENT field, thereby counting the number of hosts being the NAT
- Part b) The IDENT field is randomly assigned the above method would not work, instead the number of unique IDENT's should be counted to identify the number of hosts behind a NAT

6.2 ICMP and Ping

Problem 1

Part a) Host IP addr. : 172.16.199.132.

Part b) Dest IP addr. : 143.89.14.2.

Part c) ICMP protocol No.: 1.

Part d) ICMP is not an application layer protocol, and only communicates between hosts and routers.

Part e) ICMP type: 8 and code: 0. The type indicates that this ICMP is a ping request and the code means ??

Part f) Sequence No.: (BE)1, (LE)256. Identifier: (BE):1846, (LE):13831. The sequence number and identifier are used to match responses to their request.

Problem 2

Part a) Type: 0, Code: 0. This pair of values correspond to a ICMP ping reply message

Part b) Sequence Number: (BE)1 & (LE) 256, Identifier: (BE)1846 & (LE)13831. The sequence number and identifier are used to match responses to their request.

Figure 1: The console output of the ping to ust.hk

```
root@kali:~# wireshark&
[1] 61438
root@kali:~# ping -c 10 www.ust.hk
PING www.ust.hk (143.89.14.2) 56(84) bytes of data:
64 bytes from www.ust.hk (143.89.14.2): icmp_seq=1 ttl=128 time=241 ms
64 bytes from www.ust.hk (143.89.14.2): icmp_seq=2 ttl=128 time=239 ms
64 bytes from www.ust.hk (143.89.14.2): icmp_seq=3 ttl=128 time=239 ms
64 bytes from www.ust.hk (143.89.14.2): icmp_seq=4 ttl=128 time=239 ms
64 bytes from www.ust.hk (143.89.14.2): icmp_seq=5 ttl=128 time=239 ms
64 bytes from www.ust.hk (143.89.14.2): icmp_seq=6 ttl=128 time=239 ms
64 bytes from www.ust.hk (143.89.14.2): icmp_seq=7 ttl=128 time=241 ms
64 bytes from www.ust.hk (143.89.14.2): icmp_seq=8 ttl=128 time=239 ms
64 bytes from www.ust.hk (143.89.14.2): icmp_seq=9 ttl=128 time=239 ms
64 bytes from www.ust.hk (143.89.14.2): icmp_seq=10 ttl=128 time=239 ms

--- www.ust.hk ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9015ms
rtt min/avg/max/mdev = 239.115/239.701/241.488/0.987 ms
root@kali:~#
```

Figure 2: The first ICMP packet

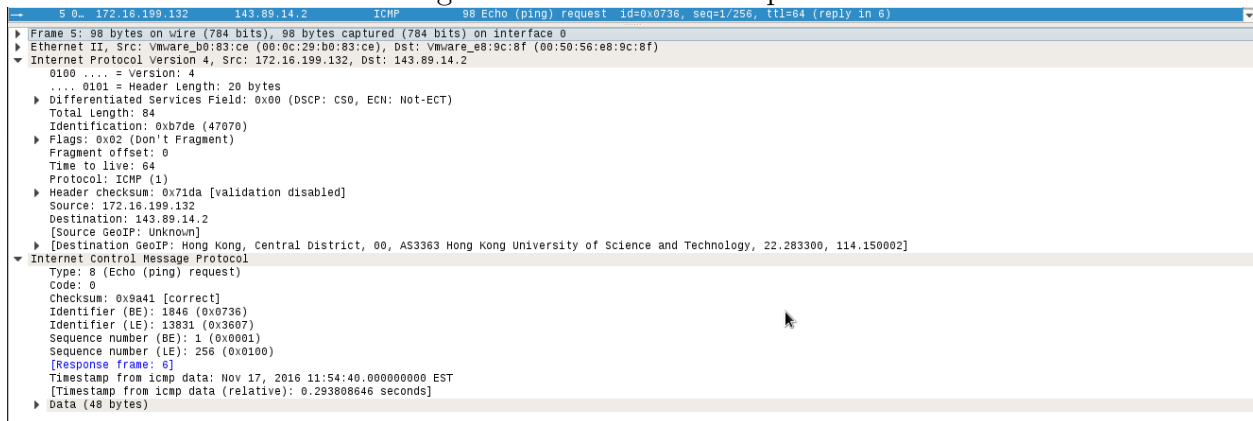
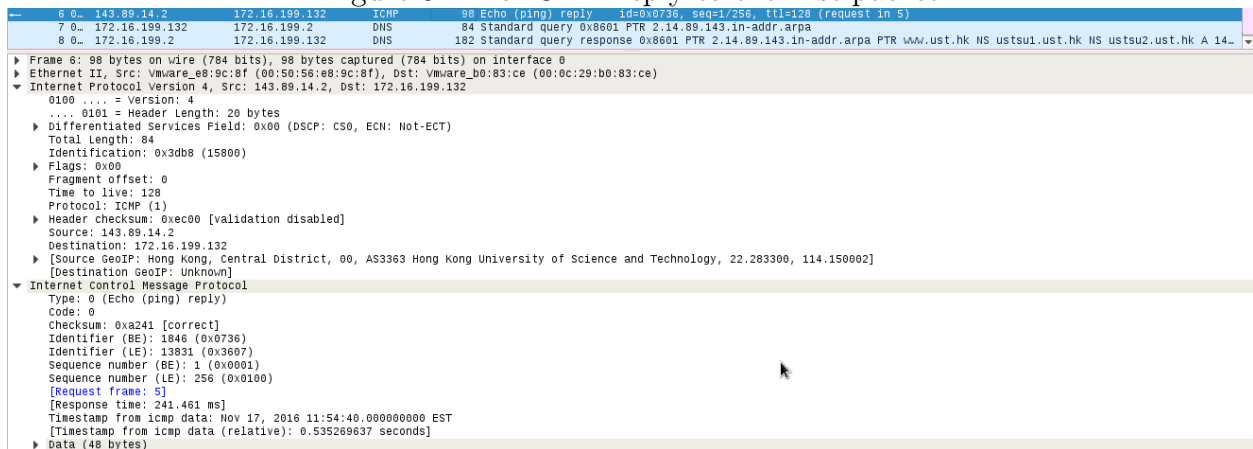


Figure 3: The ICMP reply to the first packet



6.3 ICMP and Traceroute

Problem 1

Part a) Host IP addr.: 172.16.199.132.

Part b) Dest IP addr.: 222.92.46.5.

Part c) UDP protocol No.: 17.

Part d) TTL field value: 1

Problem 2 The fourth UDP packet had a TTL of 2.

Problem 3 The ICMP TTL-exceeded error has type 11, code 0 field values

Problem 4 ??

Figure 4: The first UDP packet

7	2.	172.16.199.132	222.92.46.5	UDP	74 54262 - 33434	Len=32
8	2.	172.16.199.132	222.92.46.5	UDP	74 50829 - 33435	Len=32
9	2.	172.16.199.2	172.16.199.132	ICMP	102 Time-to-live exceeded (Time to live exceeded in transit)	
10	2.	172.16.199.2	172.16.199.132	ICMP	102 Time-to-live exceeded (Time to live exceeded in transit)	
11	2.	172.16.199.132	222.92.46.5	UDP	74 54485 - 33436	Len=32
12	2.	172.16.199.132	222.92.46.5	UDP	74 55676 - 33437	Len=32
13	2.	172.16.199.2	172.16.199.132	ICMP	102 Time-to-live exceeded (Time to live exceeded in transit)	
14	2.	172.16.199.132	222.92.46.5	UDP	74 42090 - 33438	Len=32
15	2.	172.16.199.132	222.92.46.5	UDP	74 51927 - 33439	Len=32
16	2.	172.16.199.132	222.92.46.5	UDP	74 46812 - 33440	Len=32
17	2.	172.16.199.132	222.92.46.5	UDP	74 34520 - 33441	Len=32
18	2.	172.16.199.132	222.92.46.5	UDP	74 38464 - 33442	Len=32
19	2.	172.16.199.132	222.92.46.5	UDP	74 41868 - 33443	Len=32
20	2.	172.16.199.132	222.92.46.5	UDP	74 34001 - 33444	Len=32
21	2.	172.16.199.132	222.92.46.5	UDP	74 41363 - 33445	Len=32

▶ Frame 7: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
 ▶ Ethernet II, Src: Vmware_b0:83:ce (00:0c:29:b0:83:ce), Dst: Vmware_e8:9c:8f (00:50:56:e8:9c:8f)
 ▶ Internet Protocol Version 4, Src: 172.16.199.132, Dst: 222.92.46.5
 0100 = Version: 4
 0101 = Header Length: 20 bytes
 ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 60
 Identification: 0x9bbc (39868)
 ▶ Flags: 0x00
 Fragment offset: 0
 ▶ Time to live: 1
 Protocol: UDP (17)
 ▶ Header checksum: 0x9dfe [validation disabled]
 Source: 172.16.199.132
 Destination: 222.92.46.5
 [Source GeoIP: Unknown]
 ▶ [Destination GeoIP: China, Nanjing, 04, AS4134 Chinanet, 32.061699, 118.777802]

Figure 5: The fourth UDP packet

12	2.	172.16.199.132	222.92.46.5	UDP	74 55676 - 33437	Len=32
13	2.	172.16.199.2	172.16.199.132	ICMP	102 Time-to-live exceeded (Time to live exceeded in transit)	
14	2.	172.16.199.132	222.92.46.5	UDP	74 42090 - 33438	Len=32
15	2.	172.16.199.132	222.92.46.5	UDP	74 51927 - 33439	Len=32
16	2.	172.16.199.132	222.92.46.5	UDP	74 46812 - 33440	Len=32
17	2.	172.16.199.132	222.92.46.5	UDP	74 34520 - 33441	Len=32
18	2.	172.16.199.132	222.92.46.5	UDP	74 38464 - 33442	Len=32
19	2.	172.16.199.132	222.92.46.5	UDP	74 41868 - 33443	Len=32
20	2.	172.16.199.132	222.92.46.5	UDP	74 34001 - 33444	Len=32
21	2.	172.16.199.132	222.92.46.5	UDP	74 41363 - 33445	Len=32

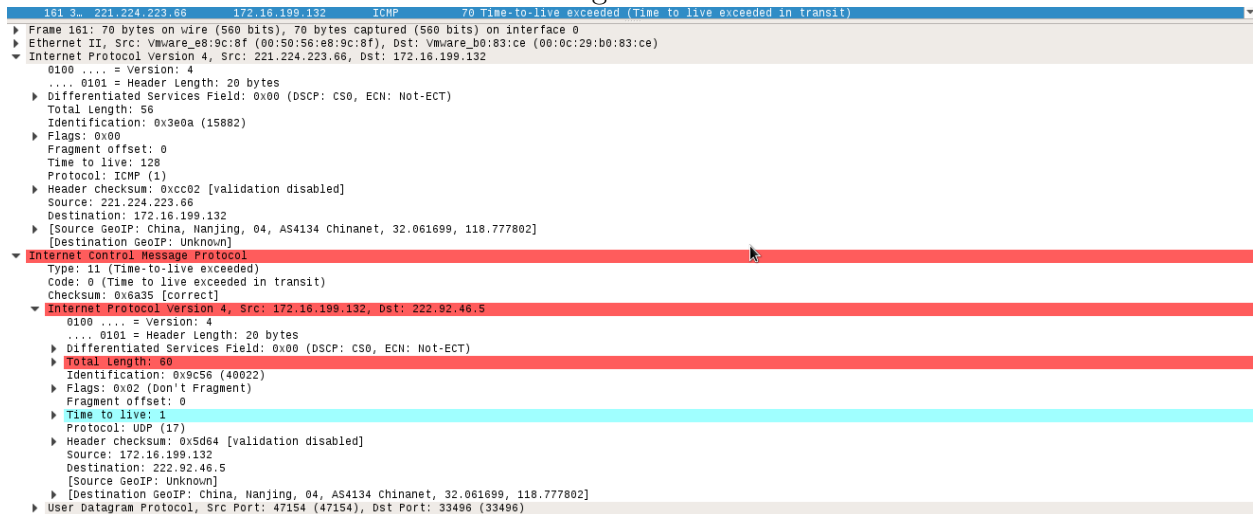
▶ Frame 12: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
 ▶ Ethernet II, Src: Vmware_b0:83:ce (00:0c:29:b0:83:ce), Dst: Vmware_e8:9c:8f (00:50:56:e8:9c:8f)
 ▶ Internet Protocol Version 4, Src: 172.16.199.132, Dst: 222.92.46.5
 0100 = Version: 4
 0101 = Header Length: 20 bytes
 ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 60
 Identification: 0x9bbf (39871)
 ▶ Flags: 0x00
 Fragment offset: 0
 ▶ Time to live: 2
 Protocol: UDP (17)
 ▶ Header checksum: 0x9cfb [validation disabled]
 Source: 172.16.199.132
 Destination: 222.92.46.5
 [Source GeoIP: Unknown]
 ▶ [Destination GeoIP: China, Nanjing, 04, AS4134 Chinanet, 32.061699, 118.777802]

Figure 6: The ICMP TTL-exceeded packet

9	2.	172.16.199.2	172.16.199.132	ICMP	102 Time-to-live exceeded (Time to live exceeded in transit)	
---	----	--------------	----------------	------	--	--

▶ Frame 9: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface 0
 ▶ Ethernet II, Src: Vmware_e8:9c:8f (00:50:56:e8:9c:8f), Dst: Vmware_b0:83:ce (00:0c:29:b0:83:ce)
 ▶ Internet Protocol Version 4, Src: 172.16.199.2, Dst: 172.16.199.132
 0100 = Version: 4
 0101 = Header Length: 20 bytes
 ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 88
 Identification: 0x3dc5 (15813)
 ▶ Flags: 0x00
 Fragment offset: 0
 Time to live: 128
 Protocol: ICMP (1)
 ▶ Header checksum: 0x1638 [validation disabled]
 Source: 172.16.199.2
 Destination: 172.16.199.132
 [Source GeoIP: Unknown]
 [Destination GeoIP: Unknown]
 ▶ Internet Control Message Protocol
 Type: 11 (Time-to-live exceeded)
 Code: 0 (Time to live exceeded in transit)
 Checksum: 0x7530 [correct]
 ▶ Internet Protocol Version 4, Src: 172.16.199.132, Dst: 222.92.46.5
 0100 = Version: 4
 0101 = Header Length: 20 bytes
 ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 60
 Identification: 0x9bbc (39868)
 ▶ Flags: 0x00
 Fragment offset: 0
 ▶ Time to live: 1
 Protocol: UDP (17)
 ▶ Header checksum: 0x9dfe [validation disabled]
 Source: 172.16.199.132
 Destination: 222.92.46.5
 [Source GeoIP: Unknown]
 ▶ [Destination GeoIP: China, Nanjing, 04, AS4134 Chinanet, 32.061699, 118.777802]
 ▶ User Datagram Protocol, Src Port: 54262 (54262), Dst Port: 33434 (33434)
 ▶ Data (32 bytes)

Figure 7:



6.4 Fragmentation

Problem 1 No fragments and as no packet as the MF field set.

Problem 2 Yes, the MF bit is set and the 1st packet. There are 2 fragments in the form of UDP packets

Problem 3 Yes, there are 3 fragments.

Problem 4 The MF field is set and the length of the packet is of maximum size. Also, the offset is 0.

Problem 5 The MF field is 1 and the offset is 1480.

Problem 6 The offset and the checksum.

Problem 7 All Flags are set to 0 and the sum of the offset and packet length adds to the original datagram size.

Problem 8 The MTU of the network is 1500 bytes.

Figure 8: Console output for ping with datagram of 1000B

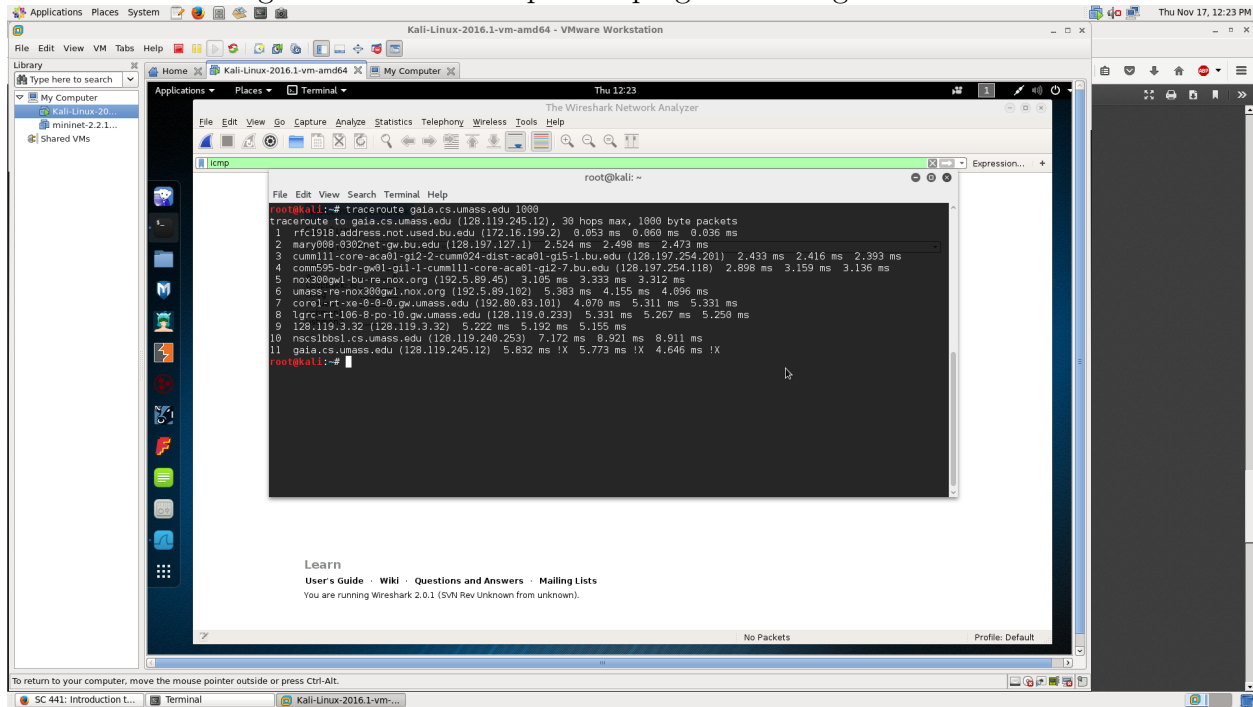


Figure 9: Console output for ping with datagram of 2000B

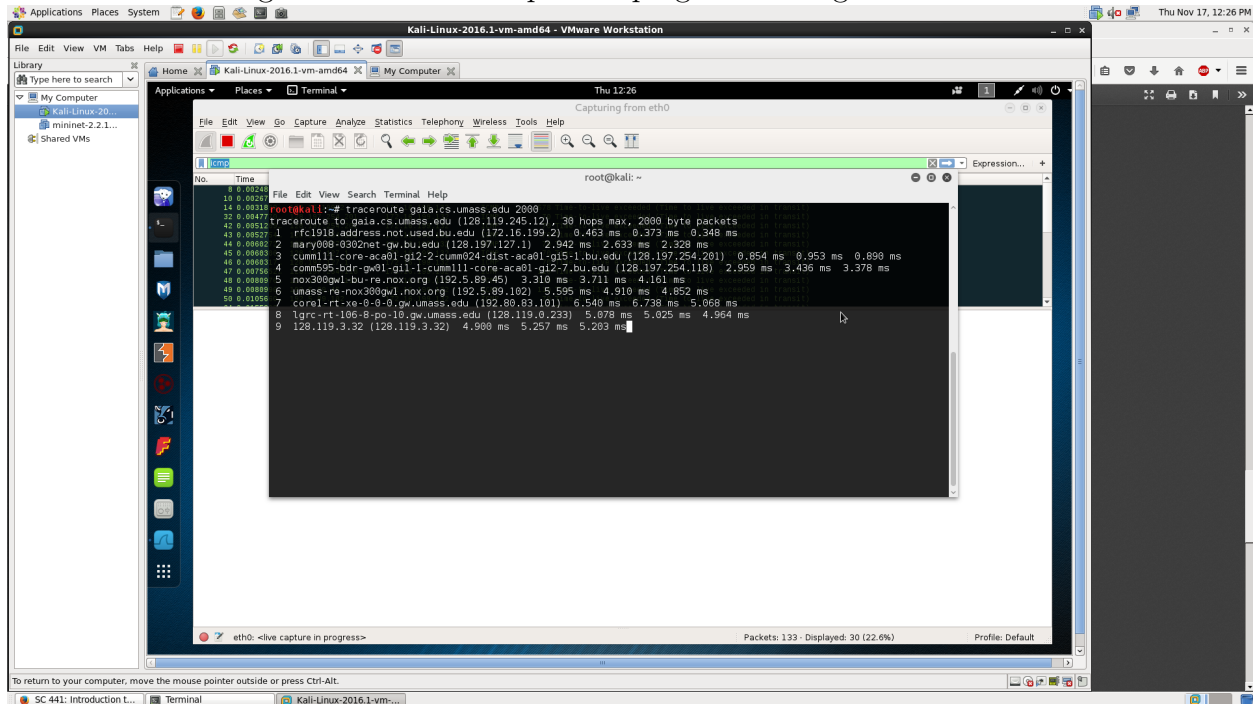


Figure 10: Console output for ping with datagram of 3500B

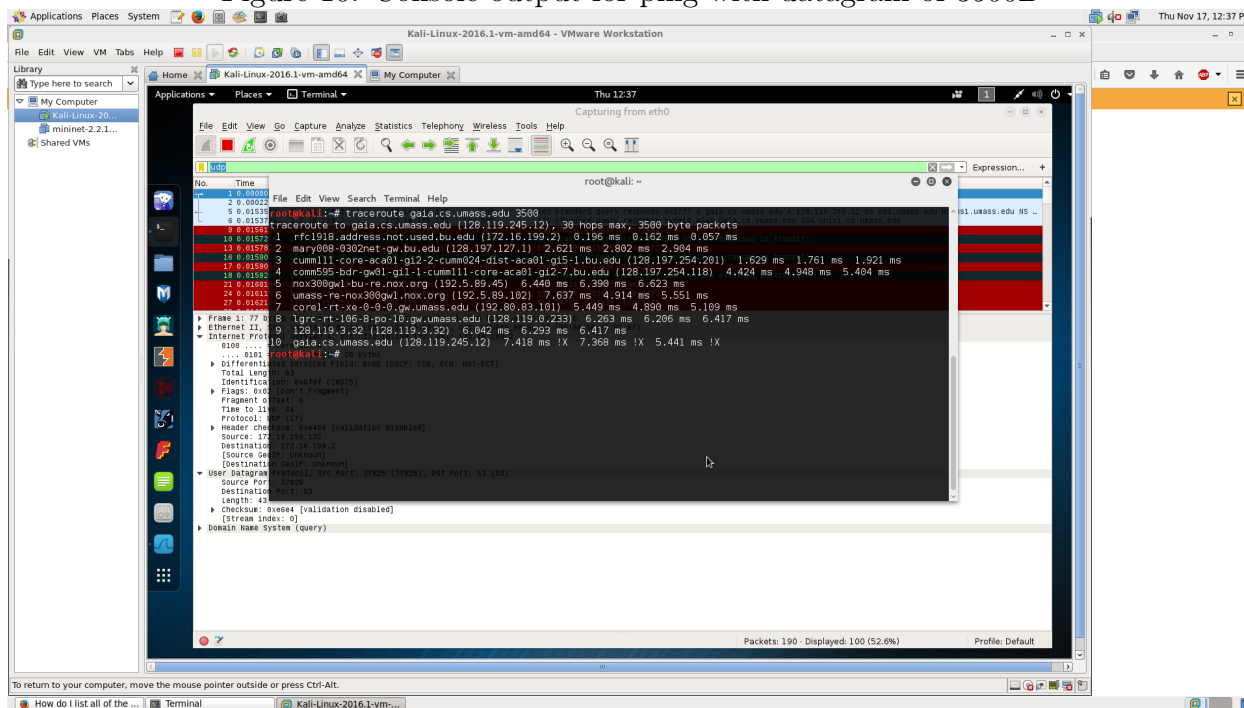


Figure 11: First UDP probe

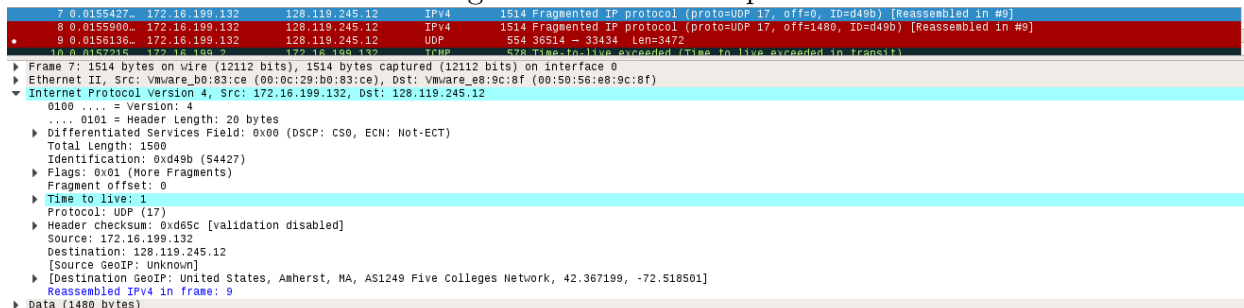


Figure 12: Second UDP fragment

